EXHIBIT
F

FILED VIA EFS WEB

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT

Applicants:	Bennau, Blayn W.	Docket No.:	12655.1600
Serial No.:	12/512,873	Examiner:	Reagan, James W.
Filed:	July 30, 2009	Group Art Unit:	3621
Title:	METHODS, APPARATUS, AND COMPUTER PROGRAM PRODUCTS FOR SECURELY ACCESSING ACCOUNT DATA	Confirmation No.:	6515

AMENDMENT AND REPLY

Mail Stop AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Commissioner:

In reply to the Final Office Action dated January 26, 2011, of which this Reply is filed within two months, please amend the above-identified application as follows:

Amendments to the Claims begin on page 2 of this paper.

Remarks/Arguments begin on page 8 of this paper.

Amendments to Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method comprising:

receiving, by a computer-based system for securely downloading customer data to a browser toolbar and via the browser toolbar, a request for customer data from a customer;

determining, by the computer-based system, that the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;

authenticating, by the computer-based system, the customer based on a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer;

encrypting, by the computer-based system, the requested personal identifiable information using the public encryption key generated by the browser toolbar; and

transmitting, by the computer-based system, the encrypted personal identifiable information to the browser toolbar,

wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet).

2. (Original) The method of claim 1, further comprising:

analyzing, by the browser toolbar, web services initiated on a computer system executing the browser toolbar;

detecting, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and

creating a public/private key pair combination in response to the detecting.

3. (Original) The method of claim 1, wherein the account specific access credential includes a card security code associated with the customer.

4. (Previously presented) The method of claim 1, further comprising:

determining, by the computer-based system, that the account of the customer is eligible for use with a web service initiating the request for customer data;

retrieving, by the computer-based system, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account from another; and

transmitting, by the computer-based system, the generic account data to a computer system executing the browser toolbar.

5. (Previously presented) The method of claim 4, wherein the generic account data includes a portion of an account number associated with the account of the customer.

6. (Previously presented) The method of claim 4, further comprising:

receiving, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and

determining whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential.

7. (Cancelled)

8. (Currently amended) A system comprising:

a tangible, non-transitory memory communicating with a processor for securely integrating personal identifiable information with a browser toolbar,

the tangible, non-transitory memory having instructions stored thereon that, in response to execution by the processor, cause the processor to perform operations comprising:

receiving, by the processor, via the browser toolbar, a request for customer data from a customer;

determining, by the processor, that the request for customer data includes a request for personal identifiable information requiring encryption with a public encryption key generated by the browser toolbar;

authenticating, by the processor, the customer based on a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer;

encrypting, by the processor, the requested personal identifiable information using the public encryption key generated by the browser toolbar; and

transmitting, by the processor, the encrypted personal identifiable information to the browser toolbar,

wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet).

9. (Previously presented) The system of claim 8, wherein the browser toolbar is further configured to:

analyze web services initiated on a computer system executing the browser toolbar;

detect when the request for customer data includes the request for personal identifiable information; and

create a public/private key pair combination.

10. (Previously presented) The system of claim 8, wherein the account specific access credential includes a card security code associated with the customer.

11. (Currently amended) The system of claim 8, further comprising:

determining, by the processor, that the account of the customer is eligible for use with a web service initiating the request for customer data;

retrieving, by the processor, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account of the customer from another; and transmitting, by the processor[[,]], via the transmission unit, the generic account data to a computer system executing the browser toolbar.

12. (Previously presented) The system of claim 11, wherein the generic account data includes a portion of an account number associated with the account of the customer.

13. (Previously presented) The apparatus of claim 11, wherein the toolbar server application is further configured to:

receive, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and

determine whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential.

14. (Currently amended) An article of manufacture including a non-transitory, tangible computer readable medium having instructions stored thereon that, in response to execution by a computer-based system for securely downloading customer data to a browser toolbar, cause the computer-based system to perform operations comprising:

receiving, by the computer-based system and via the browser toolbar, a request for customer data from a customer;

determining, by the computer-based system, that the request for customer data includes a request for personal identifiable information requiring encryption by a public encryption key generated by the browser toolbar;

authenticating, by the computer-based system, the customer based on a user credential and an account specific access credential, wherein:

the user credential and the account specific access credential are distinct, and

the account specific access credential is associated with an account of the customer;

encrypting, by the computer-based system, the requested personal identifiable information using the public encryption key generated by the browser toolbar; and transmitting, by the computer-based system, the encrypted personal identifiable information to the browser toolbar,

wherein the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet).

15. (Previously presented) The article of Claim 14, further comprising:

analyzing, by the browser toolbar, web services initiated on a computer system executing the browser toolbar;

detecting, by the browser toolbar, based at least in part on the analyzing, when the request for customer data includes the request for personal identifiable information; and

creating, by the browser toolbar, a public/private key pair combination in response to the detecting.

16. (Previously presented) The article of Claim 14, wherein the account specific access credential includes a card security code associated with the customer.

17. (Previously presented) The article of Claim 14, further comprising:

determining, by the computer-based system, that the account of the customer is eligible for use with a web service initiating the request for customer data;

retrieving, by the computer-based system, generic account data associated with the account of the customer, wherein the generic account data includes information for the customer to decipher the account of the customer from another; and

transmitting, by the computer-based system, the generic account data to a computer system executing the browser toolbar.

18. (Previously presented) The article of Claim 17, wherein the generic account data includes a portion of an account number associated with the account of the customer.

19. (Previously presented) The article of Claim 14, further comprising:

receiving, by the computer-based system, via a user interface, a selection request indicating the customer requests access to personal identifiable information associated with the account of the customer; and determining, by the computer-based system, whether the customer has access to the personal identifiable information associated with the account of the customer based at least in part on the account specific access credential.

20. (Cancelled)

Remarks

Applicants reply to the Final Office Action dated January 26, 2011 within two months. The Examiner rejects claims 1-20. Claims 7 and 20 are cancelled without prejudice or disclaimer. Support for the amendments may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments. Applicants assert that the application is in condition for allowance and reconsideration is requested.

Applicants thank the Examiner for the telephone interview of March 17, 2011. Applicants summarize the contents of the interview for the Examiner's convenience. Applicants discussed with the Examiner the purpose of the system, which is to safeguard a user's data from theft/attack after the data is downloaded and decrypted by the user's computer, and before the user is permitted access to the data. To this end, Applicants clarified that the system saves the decrypted data to a secure e-wallet prior to giving a user access to the data, thereby preventing the data from being accessed by rogue programs running on the user's device (as per paragraph [0007] of the originally-filed specification). The Examiner agreed that an amendment reciting a similar limitation would aid prosecution and likely overcome at least the reference Reno (see below).

Rejections Under 35 U.S.C. §103(a)

The Examiner rejects claims 1-6 and 8-19 under 35 U.S.C. §103(a) as being unpatentable over Reno et al., U.S. Published Application No. 2005/0172229 ("Reno") in view of Weber, U.S. Published Application No. 2004/0061720 ("Weber"). The Examiner further rejects claims 7 and 20 under 35 U.S.C. §103(a) in view of Reno further in view of Weber and further in view of Official Notice. Applicants respectfully disagree with the Examiner's rejections; however Applicants amend certain pending claims, without prejudice or disclaimer, to clarify the patentable aspects and to expedite prosecution.

Reno is directed to a browser user-interface security application that is configured to transmit sensitive information (e.g., an account number, a user name and password) to a bank system (para. [0034], lines 11-13). The purpose of the Reno system is to safeguard an account holder from entering his account number, user name, and password in a fraudulent or "spoofed" bank website (Figs. 3A and 3B, para. [0003]). Hence, Reno discloses using an encryption technique (i.e., SSL/TSL) to encrypt an account holder's sensitive information (i.e., account number, user name, and password) at a client machine. The sensitive information is decrypted at a bank server (para. [0031], para. [0036]), and a user is given access to his bank account.

Applicants now reiterate an important distinction between Reno and the pending claims (see also interview summary above). Referring to Applicants' specification, Applicants describe at paras. [0006]-[0009] an "e-wallet" or digital wallet which may facilitate payment for purchases made online. However, Applicants note that prior art e-wallets have the disadvantage that, "[e]ven if account data is ultimately stored in an encrypted form, the account data may be exposed during data entry and prior to encryption by the digital wallet software." Thus, Applicants explain that there are prior art systems which permit users to view some of their financial account information —e.g., some systems permit users to log into their bank accounts to view account information (e.g., Reno). However, what has been lacking is an ability to access "customer account data for transaction processing." In other words, what has been lacking is an e-wallet that is secure from attack after account data is downloaded, but before a user is given access to the data. The pending application solves this problem by generating an encryption key by the e-wallet (i.e., the browser toolbar), such that when a request is made by the browser toolbar for account information, the account information is encrypted at a transaction account issuer/bank system using the encryption key provided by the e-wallet. Further, on receipt of encrypted data, the browser toolbar may decrypt and save the data to a secure e-wallet prior to giving a user access to the data, thereby preventing attacks on the data by rogue programs running on the user's system.

Therefore, Applicants respectfully submit that Reno fails to disclose or contemplate, at least, "**the encrypted personal identifiable information is decrypted by the browser toolbar and saved to a secure electronic wallet (e-wallet),**" as similarly recited by independent claims 1, 8, and 14 (emphasis added).

Weber discloses a multi-function browser toolbar that allows a user to "toggle groups of online search engines specializing in a specific field" (Abstract). For instance, with reference to Figures 1A-1D, Weber discloses a toolbar that permits toggling between one or more search engines (Fig. 1A), one or more subject (Fig. 1C), and/or one or more websites (Fig. 1D). Applicants therefore respectfully submit that Weber fails to remedy the deficiencies described above.

The Examiner asserts that "electronic purses and wallets" were old and well known at the time of invention. Accordingly, the Examiner asserts that it would have been obvious to "combine/modify the method of **RENO/WEBER** with the technique of an e-wallet, because 'Fraudulent activities on the Internet have increased drastically'" (citing Reno). As discussed above and during the recent interview, although e-wallets may have been known in the art at the time of invention, it would not have been obvious to combine an e-wallet with Reno or Reno-Weber, because Reno is not directed to securing personal identifiable information (e.g., data that a user may use to make a purchase online) after a secure download from a server and before use/access by a user. Rather, Reno focuses on reducing the likelihood that a user will provide sensitive information to a spoofed website (para. [0019]). That is, **although Reno may disclose secure (e.g., SSL/TSL) transmission of sensitive information to a browser, in fact the Reno system suffers from a vulnerability remedied by Applicants and not contemplated by Reno (i.e., vulnerability of decrypted information to attack by rogue programs on the user's computer)** (see originally-filed specification at para. [0007]). Moreover, Reno is concerned with logging a user into his bank account (see Figs. 3A-3B), as opposed to enabling a user to make purchases via a secure file (i.e., an e-wallet) saved on the user's computer. Thus, it would not have been obvious to a person of ordinary skill to add an e-wallet to Reno or Reno-Weber, for the additional reason that Reno does not actually contemplate enabling a user to make a purchase using downloaded account information. That is, Reno merely gives access to a bank account (e.g., a Bank of America account, as illustrated by Figs. 3A-3B).

Applicants therefore respectfully assert that independent claims 1, 8, and 14 are allowable over the cited references. Claims 2-6, 9-13, and 15-19 variously depend from independent claims 1, 8, and 14. As such, Applicants assert that claims 2-6, 9-13, and 15-19 are differentiated from the cited references for the same reasons as set forth above, in addition to their own novel features. Applicants therefore respectfully request allowance of all of the pending claims.

When a phrase similar to "at least one of A, B, or C" or "at least one of A, B, and C" is used in the claims or specification, Applicants intend the phrase to mean any of the following: (1) at least one of A; (2) at least one of B; (3) at least one of C; (4) at least one of A and at least one of B; (5) at least one of B and at least one of C; (6) at least one of A and at least one of C; or (7) at least one of A, at least one of B, and at least one of C.

Applicants respectfully submit that the pending claims are in condition for allowance. The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. **19-2814**. **This statement does NOT authorize charge of the issue fee.** If an extension of time is necessary, please accept this as a petition therefore. Applicants invite the Office to telephone the undersigned if the Examiner has any questions regarding this Reply or the present application in general.

Respectfully submitted,

Dated: 3/21/2011

By: ______________________
/James Henson
Reg. No. 65,118

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6396
Fax: 602-382-6070
Email: jhenson@swlaw.com